PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM Internationales Büro INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7: (11) Internationale Veröffentlichungsnummer: WO 00/63827 G06K 7/00 A1 (43) Internationales Veröffentlichungsdatum: 26. Oktober 2000 (26.10.00)

(21) Internationales Aktenzeichen:

PCT/EP00/03429

(22) Internationales Anmeldedatum:

14. April 2000 (14.04.00)

(30) Prioritätsdaten:

99107578.9

15. April 1999 (15.04.99)

(71) Anmelder (für alle Bestimmungsstaaten ausser US): INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Str. 53, D-81541 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): WEDER, Uwe [DE/DE]; Im Bäckerfeld 23 A, D-84072 Au/Hallertau (DE).

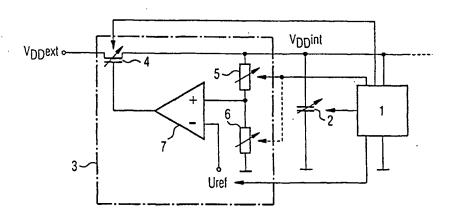
(74) Gemeinsamer Vertreter: INFINEON TECHNOLOGIES AG; Zedlitz, Peter, Postfach 22 13 17, D-80503 München (DE). (81) Bestimmungsstaaten: BR, CN, IN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht

Mit internationalem Recherchenbericht.

(54) Title: INTEGRATED CIRCUIT WITH A CONTROLLABLE VOLTAGE REGULATOR

(54) Bezeichnung: INTEGRIERTE SCHALTUNG MIT STEUERBAREM SPANNUNGSREGLER



(57) Abstract

Disclosed is a circuit integrated on a semiconductor-chip. The aim of the invention is to hide the current profile which can be detected on the input terminal of the supply voltage. To this end, the characteristics of a voltage regulator can be changed.

(57) Zusammenfassung

Es wird eine auf einem Halbleiter-Chip integrierte Schaltung beschrieben, bei der eine Verschleierung des an einer Versorgungsspannungseingangsklemme detektierbaren Stromprofils durch einen in seinen Eigenschaften anderbaren Spannungsregler erreicht wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

Al	L	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
A.	M	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
A'	T	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
A	U	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
A:	Z	Aserbaidschan	. GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
В	A	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
В	В	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
В	E	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische	TM	Turkmenistan
B	F	Burkina Faso	GR	Griechenland		Republik Mazedonien	TR	Türkei
В	G	Bulgarien	HU	Ungam	ML	Mali	TT	Trinidad und Tobago
В.	J	Benin	ΙE	Irland	MN	Mongolei	UA	Ukraine
В	R	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
В	Y	Belarus	IS	Island	· MW	Malawi	US	Vereinigte Staaten von
С	A	Kanada	IT	Italien	MX	Mexiko		Amerika
С	F	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
С	:G	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
· C	H	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
С	1	Côte d'Ivoire	KP	Demokratische Volksrepublik	NZ	Neuseeland	zw	Zimbabwe
C	M	Kamerun		Korea	PL	Polen		
С	N	China	KR	Republik Korea	PT	Portugal		
C	Ü	Kuba	KZ	Kasachstan	RO	Rumānien		
С	Z	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation	:	
D	E	Deutschland	LI	Liechtenstein	SD	Sudan		
D	K	Dänemark	LK	Sri Lanka	SE	Schweden		
E	E	Estland	LR	Liberia	SG	Singapur .		
İ								

1

Beschreibung

30

Integrierte Schaltung mit steuerbarem Spannungsregler

5 Integrierte Schaltungen insbesondere solche zur Verwendung in tragbaren Datenträgern wie Chipkarten bieten viele Manipulations- und/oder Analyseanreize, da sie zunehmend in sicherheitskritischen Bereichen wie Zutrittskontrolle, als wiederaufladbare Geldkarte oder zur Erzeugung elektronischer Unterschriften eingesetzt werden.

Die für die Sicherheit der genannten Anwendungen maßgeblichen Elemente sind zumeist speziell konfigurierte Schaltungsteile oder in nicht-flüchtigen Speichern abgelegte geheime Informa-15 tionen. Um ein Ausspähen dieser Details zu verhindern wurde in der Vergangenheit vorgeschlagen, Schaltungsteile in tieferen Ebenen der integrierten Schaltung zu realisieren, so daß durch darüberliegende Strukturen verdeckt sind. Andere Vorschläge zielten auf eine zusätzliche vorzugsweise leitende Abdeckung der integrierten Schaltung, die in die Stromversor-. gung einbezogen ist und deren Vorhandensein bzw. Unversehrtheit detektiert werden kann, um den Verarbeitungsablauf in der integrierten Schaltung entsprechend zu beeinflussen. Darüberhinaus ist auch schon eine Verschlüsselung des Datenaus-25 tauschs zwischen Bestandteilen einer Schaltung auf einem einzigen Halbleiterchip vorgeschlagen worden.

All diese Schutzmaßnahmen greifen jedoch nicht in ausreichendem Maße bei einer seit einiger Zeit bekanntgewordenen Analysemethode, die sich auf die Beobachtung und statistische Auswertung des von außen meßbaren Strukturprofils bei bestimmungsgemäßem Gebrauch beschränkt, ohne also den Halbleiterchip zu verändern. Diese Methode ist unter der englischen Bezeichnung Differential Power Analysis bekannt geworden und eine kurze Beschreibung dieser Methode ist beispielsweise in der Internet-Seite http://www.cryptography.com veröffentlicht.

PCT/EP00/03429 WO 00/63827

2

Danach hat es sich gezeigt, daß bei gleichen Abläufen innerhalb der integrierten Schaltung - beispielsweise bei Ausführung des gleichen Befehls in einem Mikroprozessor - das gleiche Stromprofil an der Versorgungsspannungseingangsklemme meßbar ist. Durch statistische Auswertung dieses Stromprofils können sogar einzelne Bits einer für eine Verschlüsselung erforderlichen geheimen Zahl ermittelt werden.

10 Die Aufgabe vorliegender Erfindung ist es, einen Schutz vor einer solchen Analyse zu bieten.

Die Aufgabe wird durch eine auf einem Halbleiterchip integrierte Schaltung mit dem Merkmal des Anspruchs 1 gelöst.

Vorteilhafte Weiterbildungen sind in den Unteransprüchen an-15 gegeben.

Die erfindungsgemäße integrierte Schaltung weist also einen Versorgungsspannungsregler auf, der prinzipiell die Spannung an einem Ladungsspeicher, insbesondere einem Pufferkondensator, stabilisieren soll. Der Ladungsspeicher kann aber auch bereits durch die Kapazität der integrierten Schaltung selbst gegeben sein. Dieser Spannungsregler arbeitet aber nicht konstant auf einem Arbeitspunkt sondern wird durch eine Steuer-25 einheit in seinen Regeleigenschaften verändert. Hierdurch werden die durch den Datenverarbeitungsteil der integrierten Schaltung erzeugten Stromprofilschwankungen durch die vom Spannungsregler stammenden Schwankungen überlagert, so daß das tatsächliche Stromprofil verschleiert wird und somit bei 30 gleichen Verarbeitungsvorgängen innerhalb der integrierten Schaltung aufgrund der Änderungen der Parameter der Regelschaltung unterschiedliche Stromprofile resultieren und somit kein Zusammenhang zwischen Stromprofil und Verarbeitungsvorgang mit statistischen Methoden hergeleitet werden kann.

35

20

In einer Variante der Erfindung wird statt oder zusätzlich zu dem Spannungsregler die Kapazität des Ladungsspeichers geän-

3

dert. Dies entspricht in seiner Auswirkung dem Andern des Widerstands eines Längsregeltransistors bei einem Serienregler, da hierdurch die Zeitkonstante des durch diesen Längsregeltransistor und den Ladungsspeicher gebildeten Tiefpasses beeinflußt wird.

Um eine erfolgreiche Beeinflussung des Stromprofils zu erzielen müssen die Änderungen der Regler- bzw. Ladungsspeichereigenschaften zeitlich und hinsichtlich der Auswirkung auf die Amplitude des Stromprofils im Bereich der typischen Werte der durch schaltungsinterne Vorgänge hervorgerufenen Änderungen liegen.

Besonders vorteilhaft wirkt sich eine Änderung der internen
Versorgungsspannung zu niedrigeren Werten hin aus, die in
diesem Fall auch langsamer sein kann, da dann bei besonders
sicherheitskritischen Vorgängen die Energie allein aus dem
Ladungsspeicher bezogen werden kann, ohne daß dies im Ladestrom zu einer Profilierung führen würde. Eine Nachladung des
Ladungsspeichers kann bei nicht-sicherheitskritischen Vorgängen erfolgen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe einer Figur näher erläutert.

25

10

Die Figur zeigt eine integrierte Schaltung gemäß der Erfindung, die ein Teil einer auf einem Halbleiterchip realisierten Schaltung ist. Der nicht zur Erfindung gehörende Teil der gesamten integrierten Schaltung, die durch die interne Versorgungsspannung VDD int versorgt wird ist durch eine gepunktete Fortsetzung der Versorgungsspannungsleitung dargestellt.

Zwischen der Klemme, an die die externe Versorgungsspannung V_{DD} ext angelegt wird und dem einen Anschluß eines als Puffer-kondensator 2 ausgebildeten Ladungsspeichers ist im gewählten Ausführungsbeispiel der Längsregeltransistor 4 eines Serienspannungsreglers 3 geschaltet. Dieser wird von einem Regel-

4

verstärker 7 angesteuert. Die beiden Eingänge des Regelverstärkers 7 sind einerseits mit einer Referenzspannung Uref und andererseits mit dem Mittelabgriff eines als Ist-Spannungsmeßeinrichtung fungierenden Spannungsteilers 5, 6 verbunden. Der Spannungsteiler 5, 6 ist parallel zum Pufferkondensator 2 geschaltet. Durch diese Schaltung soll zunächst erreicht werden, daß die interne Versorgungsspannung V_{DD} int auf einem durch die Referenzspannung Uref definierten Wert gehalten wird.

10

In erfindungsgemäßer Weise sind nun sowohl der als Stellglied des Spannungsreglers fungierende Längsregeltansistor 4, die Widerstände des Spannungsteiler 5, 6, der Pufferkondensator 2 und auch die Referenzsspannung Uref änderbar ausgebildet, was durch Pfeile angedeutet ist, und können von einer Steuerschaltung 1 angesteuert werden. Die Änderbarkeit kann zum Beispiel durch Parallelschaltung zusätzlicher entsprechender Bauteile erreicht werden. Dabei genügt es prinzipiell, wenn nur eines der genannten Elemente änderbar ausgebildet ist beziehungsweise angesteuert wird. Um aber im Sinne der zu lösenden Aufgabe eine Verschleierung des tatsächlichen Stromprofils an der Eingangsklemme (VDPEXT) zu erreichen, ist es von Vorteil, wenn mehrere Möglichkeiten vorhanden sind, die abwechselnd oder auch zusammen eingesetzt werden können.

25

30

20

Die durch die Steuereinheit 1 gesteuerten Änderungen können dabei langsam sein, um zum Beispiel für bestimmte Operationen durch Verändern der Referenzspannung Uref oder des Spannungsteilers 5, 6 die interne Versorgungsspannung V_{DD}int abzusenken, so daß die Versorgung des (nicht dargestellten) Datenverarbeitungsteils der integrierten Schaltung allein aus dem Pufferkondensator 2 erfolgen kann. Dies ist bei sicherheitskritischen Datenverarbeitungsvorgängen wie beispielsweise Verschlüsselung von Interesse, da dann kein spezifisches Stromprofil an den Eingangsklemmen detektierbar ist.

5

Andererseits können auch schnelle, zufällige Veränderungen, die sich im Pegel- und Frequenzbereich der typischen Stromprofilschwankungen bewegen sinnvoll sein, um auf diese Weise der Überlagerung der tatsächlichen Schwankungen mit den aufgezwungenen eine Verschleierung zu erreichen, die eine statistische Auswertung erschwert oder gar verunmöglicht.

Ein besonderer Vorteil der erfindungsgemäßen integrierten Schaltung besteht darin, daß die Stromverschleierung nicht auf Kosten eines zusätzlichen Leistungsverbrauchs geht.

10

6

Patentansprüche

1. Auf einem Halbleiterchip integrierte Schaltung mit einer Steuereinheit (1),

5 mit einem internen Ladungsspeicher (2), an dem die interne Versorgungsspannung $(V_{DD}int)$ der integrierten Schaltung abgreifbar ist,

mit einer externen Versorgungsspannungsklemme zur Versorgung der integrierten Schaltung mit einer externen Versorgungs-

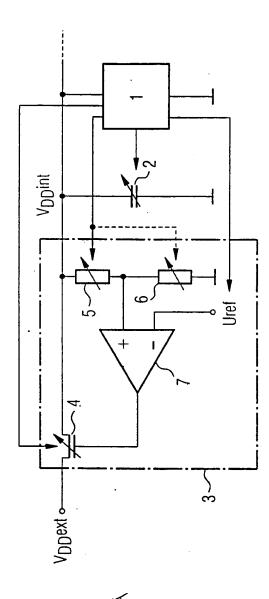
10 spannung (V_{DD}ext),

mit einem zwischen der externen Versorgungsspannungsklemme und dem Ladungsspeicher (2) angeordneten Spannungsregler (3), wobei der Spannungsregler (3) und/oder der Ladungsspeicher

- (2) mit der Steuereinheit (1) derart verbunden ist, daß Be-
- 15 triebsparameter des Spannungsreglers (3) und/oder des Ladungsspeichers (2) durch ein Steuersignal der Steuereinheit (1) änderbar ist bzw. sind.
- Integrierte Schaltung nach Anspruch 1, dadurch gekenn zeichnet, daß das Stellglied (4) des Spannungsreglers (3) durch das Steuersignal ansteuerbar ist.
- Integrierte Schaltung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Meßeinrichtung (5, 6) des Spannungsreglers (3) durch das Steuersignal ansteuerbar ist.
 - 4. Integrierte Schaltung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der Sollwert (Uref) des Spannungsreglers (3) durch das Steuersignal ansteuerbar ist.
 - 5. Integrierte Schaltung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß das Steuersignal ein Zufallssignal ist.

35

30



INTERNATIONAL SEARCH REPORT

Inte. onal Application No PCT/EP 00/03429

A CLASSIC	FICATION OF SUBJECT MATTER		······
IPC 7	G06K7/00		
According to	. International Patent Classification (IPC) or to both national classific	ation and IPC	*
B. FIELDS			
Minimum doo	currentation searched (classification system followed by classification	on symbols)	
IPC 7	G06K		,
Documentati	ion searched other than minimum documentation to the extent that s	such documents are included in the fields se	arched
Electronic da	ata base consulted during the international search (name of data ba	se and, where practical, search terms used	,
i	ternal, WPI Data, PAJ, IBM-TDB, INSE		
C. DOCUME	ENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the rel	levant passages	Relevant to claim No.
Х	US 5 479 172 A (SMITH GREGORY M 26 December 1995 (1995-12-26)	ET AL)	1-4
А	column 4, line 62 -column 11, lin figures 1-11	ne 17;	5
A	EP 0 568 398 A (GEC AVERY LTD) 3 November 1993 (1993-11-03) the whole document		1-5
			·
ш	ner documents are listed in the continuation of box C.	X Patent family members are listed	in annex.
"A" docume consid "E" earlier of filing d "L" docume which citation "O" docume other n "P" docume later th	ent which may throw doubts on priority claim(s) or is cited to establish the publication date of another in or other special reason (as specified) ent referring to an oral disclosure, use, exhibition or means ent published prior to the international filing date but is the priority date claimed.	T later document published after the inte or priority date and not in conflict with cited to understand the principle or the invention X document of particular relevance; the crannot be considered novel or cannot involve an inventive step when the document of particular relevance; the crannot be considered to involve an inventive step when the document is combined with one or moments, such combination being obvious in the art.	the application but every underlying the tairmed invention to econsidered to current is taken alone lairmed invention ventive step when the ore other such docu— us to a person skilled
Date of the	actual completion of the international search	Date of mailing of the international sea	arch report
	8 June 2000	06/07/2000	
Name and n	mailing address of the ISA European Patent Office, P.B. 5818 Patentiaan 2 NL - 2280 HV Rijswijk Tel (-31,70) 340-340-75, 31,851 moord	Authorized officer	
	Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A	· .

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte onal Application No
PCT/EP 00/03429

		<u>, </u>			00/03429
Patent document cited in search repo	ort -	Publication date	P _	atent family member(s)	Publication date
US 5479172	A	26-12-1995	NONE		
EP 0568398	Α	03-11-1993	GB	2266794 A	10-11-1993
					•
•					
	*				
					ı
			•		
				•	
				•	
		•			
					·.

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Inte onales Aktenzeichen PCT/EP 00/03429

A. KLASSIF IPK 7	izierung des anmeldungsgegenstandes G06K7/00		
Nach der Int	emationalen Patentklassifikation (IPK) oder nach der nationalen Klass	sifikation und der IPK	
	RCHIERTE GEBIETE ter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbol	a)	
IPK 7	GO6K	•,	
Recherchier	te aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, sow	weit diese unter die recherchierten Gebiete fallen	
	rinternationalen Recherche konsultierte elektronische Datenbank (Na		egriffe)
EPO-In	ternal, WPI Data, PAJ, IBM-TDB, INSP	EC .	·
CAISWE	SENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe	der in Betracht kommenden Teile	Betr. Anspruch Nr.
			· · · · · · · · · · · · · · · · · · ·
χ .	US 5 479 172 A (SMITH GREGORY M 26. Dezember 1995 (1995-12-26)	ET AL)	1-4
Α	Spalte 4, Zeile 62 -Spalte 11, Ze	ile 17;	5
	Abbildungen 1-11		
A	EP 0 568 398 A (GEC AVERY LTD)		1-5
	3. November 1993 (1993-11-03) das ganze Dokument	·	
·			
		·	
	tere Veröffentlichungen sind der Fortsetzung von Feld C zu nehmen	X Siehe Anhang Patenttamilie	
"A" Veröffe	entlichung, die den allgemeinen Stand der Technik definiert,	"T" Spätere Veröffentlichung, die nach dem inte oder dem Prioritätsdatum veröffentlicht wor	den ist und mit der
"E" äiteres	nicht als besonders bedeutsarn anzusehen ist Dokument, das jedoch erst am oder nach dem internationalen Aldedatum veröffentlicht worden ist	Anmeldung nicht kollidiert, sondem nur zun Erfindung zugrundeliegenden Prinzips oder Theorie angegeben ist	
"L" Veröffe	entlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft er-	"X" Veröffentlichung von besonderer Bedeutung kann allein aufgrund dieser Veröffentlichung erfinderischer T\u00e4tigkeit beruhend betrachte	g nicht als neu oder auf
ander soil o	ren im Recherchenbericht genannten Veröffentlichung belegt werden der die aus einem anderen besonderen Grund angegeben ist (wie	"Y" Veröffentlichung von besonderer Bedeutung kann nicht als auf erfinderischer Tätigkeit b	; die beanspruchte Erfindung
"O" Veröffe	sführt) entlichung, die sich auf eine mündliche Offenbarung, Benutzung, eine Ausstellung oder andere Maßnahmen bezieht	werden, wenn die Veröffentlichung mit eine Veröffentlichungen dieser Kategorie in Vert	r oder mehreren anderen bindung gebracht wird und
"P" Veröffe	entlichung die vor dem internationalen. Anmeldedatum, aber nach	diese Verbindung für einen Fachmann nah- "&" Veröffentlichung, die Mitglied derselben Pat	•
Datum des	Abschlusses der internationalen Recherche	Absendedatum des internationalen Recher	chenberichts
2	28. Juni 2000	06/07/2000	
Name und	Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2	Bevollmächtigter Bediensteter	
	NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichurigen, die zur selben Patentfamilie gehören

Formblatt PCT/ISA/210 (Anhang Patentfamilie)(Juli 1992)

Intel males Aktenzeichen
PCT/EP 00/03429

		PCT/EP 00/03429			
Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung 26-12-1995	Mitglied(er) der Patentfamilie KEINE		Datum der Veröffentlichung	
US 5479172 A					
EP 0568398 A	03-11-1993	GB	2266794 A	10-11-1993	
				•	
•		•			
				·	
				•	
	•				
			•		
			•		